# Vulnerability Disclosure Policy



## Introduction

The Department of Health and Human Services (HHS)is committed to ensuring the security of the American public by protecting their information from unwarranted disclosure. This policy is intended to give security researchers clear guidelines for conducting vulnerability discovery activities and to convey our preferences in how to submit discovered vulnerabilities to us.

This policy describes **what systems and types of research** are covered under this policy, **how to send us** vulnerability reports, and **how long** we ask security researchers to wait before publicly disclosing vulnerabilities.

We want security researchers to feel comfortable reporting vulnerabilities they've discovered – as set out in this policy – so we can fix them and keep our users safe. We have developed this policy to reflect our values and uphold our sense of responsibility to security researchers who share their expertise with us in good faith.

## Authorization

If you make a good faith effort to comply with this policy during your security research, we will consider your research to be authorized, we will work with you to understand and resolve the issue quickly, and HHS will not recommend or pursue legal action related to your research.

## Guidelines

Under this policy, "research" means activities in which you:

- Notify us as soon as possible after you discover a real or potential security issue.
- Make every effort to avoid privacy violations, degradation of user experience, disruption to production systems, and destruction or manipulation of data.
- Only use exploits to the extent necessary to confirm a vulnerability's presence. Do not use an exploit to compromise or exfiltrate data, establish command line access and/or persistence, or use the exploit to "pivot" to other systems.
- Provide us a reasonable amount of time to resolve the issue before you disclose it publicly.
- You do not intentionally compromise the privacy or safety of HHS personnel (e.g. civilian employees or military members), or any third parties.
- You do not intentionally compromise the intellectual property or other commercial or financial interests of any HHS personnel or entities, or any third parties.

Once you've established that a vulnerability exists or encounter any sensitive data (including personally identifiable information, financial information, or proprietary information or trade secrets of any party), **you must stop your test, notify us immediately, and not disclose this data to anyone else**.

## Scope

This policy applies to the following systems and services:

- cms.gov
- cuidadodesalud.gov
- donaciondeorganos.gov

- foodsafety.gov
- grantsolutions.gov
- healthdata.gov
- www.hhs.gov
- bhw.hrsa.gov
- bphc.hrsa.gov
- hab.hrsa.gov
- mchb.hrsa.gov
- mchbgrandchallenges.hrsa.gov
- newbornscreening.hrsa.gov
- nhsc.hrsa.gov
- poisonhelp.hrsa.gov
- insurekidsnow.gov
- medicaid.gov
- medicare.gov
- ocio.nih.gov
- organdonor.gov
- stopbullying.gov

Systems and services directly associated with domains and sub-domains listed above are in scope. Any service not expressly listed above are excluded from scope and are not authorized for testing. Additionally, vulnerabilities found in non-federal systems from our vendors fall outside of this policy's scope and should be reported directly to the vendor according to their disclosure policy (if any). If you aren't sure whether a system or endpoint is in scope or not, contact support@responsiblediscloure.com before starting your research or at the security contact for the system's domain name listed in the .gov WHOIS.

Though we develop and maintain other internet-accessible systems or services, we ask that active research and testing only be conducted on the systems and services covered by the scope of this document. If there is a system not in scope that you think merits testing, please contact us to discuss it first. We will increase the scope of this policy over time.

# Rules of Engagement

## Security researchers must not:

- Test any system other than the systems set forth in the 'Scope' section above,
- disclose vulnerability information except as set forth in the 'Reporting a Vulnerability' and 'Disclosure' sections below,
- engage in physical testing of facilities or resources,
- engage in social engineering,
- send unsolicited electronic mail to HHS users, including "phishing" messages,
- execute or attempt to execute "Denial of Service" or "Resource Exhaustion" attacks,

- introduce malicious software,
- test in a manner which could degrade the operation of HHS systems; or intentionally impair, disrupt, or disable HHS systems,
- test third-party applications, websites, or services that integrate with or link to or from HHS systems,
- delete, alter, share, retain, or destroy HHS data, or render HHS data inaccessible, or,
- use an exploit to exfiltrate data, establish command line access, establish a persistent presence on HHS systems, or “pivot” to other HHS systems.

### Security researchers may:

- View or store HHS nonpublic data only to the extent necessary to document the presence of a potential vulnerability.

### Security researchers must:

- cease testing and notify us immediately upon discovery of a vulnerability,
- cease testing and notify us immediately upon discovery of an exposure of nonpublic data, and,
- purge any stored HHS nonpublic data upon reporting a vulnerability.

## Reporting a Vulnerability

We accept vulnerability reports at https://hhs.responsibledisclosure.com . Reports may be submitted anonymously. We do not support PGP-encrypted emails at this time.

Information submitted under this policy will be used for defensive purposes only – to mitigate or remediate vulnerabilities. If your findings include newly discovered vulnerabilities that affect all users of a product or service and not solely HHS, we may share your report with the Cybersecurity and Infrastructure Security Agency, where it will be handled under their coordinated vulnerability disclosure process. We will not share your name or contact information without express permission.

By clicking “Submit Report,” you are indicating that you have read, understand, and agree to the guidelines described in this policy for the conduct of security research and disclosure of vulnerabilities or indicators of vulnerabilities related to HHS information systems, and consent to having the contents of the communication and follow-up communications stored on a U.S. Government information system.

In order to help us triage and prioritize submissions, we recommend that your reports:

- Adhere to all legal terms and conditions outlined at https://www.hhs.gov/vulnerability-disclosure-policy and the HHS Responsible Disclosure Terms of Service .
- Describe the vulnerability, where it was discovered, and the potential impact of exploitation.
- Offer a detailed description of the steps needed to reproduce the vulnerability (proof of concept scripts or screenshots are helpful).

## Disclosure

HHS is committed to timely correction of vulnerabilities. However, we recognize that public disclosure of a vulnerability in absence of a readily available corrective action likely increases versus decreases risk. Accordingly, we require that you refrain from sharing information about discovered vulnerabilities for 90 calendar days after you have received our acknowledgement of receipt of your report. If you believe others should be informed of the vulnerability prior to our implementation of corrective actions, we require that you coordinate in advance with us.

We may share vulnerability reports with the Cybersecurity and Infrastructure Security Agency (CISA), as well as any affected vendors. We will not share names or contact data of security researchers unless given explicit permission.

## Questions

Questions regarding this policy may be sent to HHS.Cybersecurity@hhs.gov. We also invite you to contact us with suggestions for improving this policy.

### HHS Headquarters

U.S. Department of Health & Human Services
200 Independence Avenue, S.W.
Washington, D.C. 20201
Toll Free Call Center: 1-877-696-6775